JOURNAL OF ALGEBRA 75, 233–260 (1982)

# A Global Code Invariant under the Higman–Sims Group*

A. R. CALDERBANK

*Department of Mathematics, Bell Laboratories, Murray Hill, New Jersey 07974*

AND

DAVID B. WALES

*Department of Mathematics, California Institute of Technology, Pasadena, California 91125*

*Communicated by Marshall Hall, Jr.*

Received December 20, 1980

## 1. INTRODUCTION

In this paper we consider certain doubly transitive permutation groups which have monomial representations which are reducible. These groups have been studied by Hale and Shult [4] and by Taylor [17]. The stabilizer $H$ of a vertex has a subgroup $L$ of index two for which elements of $L$ are not conjugate in $G$ to elements of $H - L$. The monomial representations have two invariant subspaces which can be reduced modulo any prime to form codes over finite fields. The invariant subspaces form global codes. This approach is motivated by the work of Ward [18] who considered the groups $PSL(2, q)$ and $Sp(2n, q)$. The codes for $PSL(2, q)$ give the classical extended quadratic residue codes.

In Section 2, we construct the monomial representations and determine the two invariant subspaces. Taylor constructed 2-graphs from the centralizer algebra of these representations. The invariant subspaces are spanned by vectors whose entries are parameters in these 2-graphs.

We illustrate the construction in the remaining sections with the doubly transitive permutation representation on 176 vertices of the Higman–Sims group. This permutation representation was first discovered by Graham Higman. The stabilizer of a vertex is a group $H$ isomorphic to $P\Gamma U(3, 5)$. It

* Supported in part by N.S.F. Contract MC S80-01603.



0021-8693/82/030233-28$02.00/0

has a subgroup isomorphic to $PSU(3,5)$ of index 2. The invariant subspaces of the monomial representation have dimensions 22 and 154. The 175 vertices moved by $H$ are the edges of the Hoffman–Singleton graph on 50 vertices. A set of 100 cocliques each of size 15 was found in the Hoffman–Singleton graph. These are interesting configurations in themselves. With each coclique is associated a vector in the 176-dimensional space. These 100 vectors are permuted by the monomial matrices. This permutation representation gives the original rank three construction of D. Higman and C. Sims.

The reduction modulo two for the 22-dimensional subspace gives a 22-dimensional code over $GF(2)$. The weight enumerator was computed by Neil Sloane at Bell Laboratories. There are 176 vectors of minimum weight 50. The support of a vector of minimum weight is a block in a 2-(176, 50, 14) design first discovered by G. Higman. These vectors span the space. It is remarkable that when the row space of the incidence matrix of this design is reduced modulo 2, the vectors of minimum weight are precisely the blocks of the design.

## 2. A Class of Doubly Transitive Groups and an Invariant Code

Let $G$ be a doubly transitive permutation group acting faithfully on a set $\Omega$ of size $n \geqslant 3$. Let $a \in \Omega$ and let $H = G_a$ be the stabilizer in $G$ of $a$. We shall suppose that $H$ has a normal subgroup $L$ of index 2.

Let $\varphi$ and 7 be the characters of $H$ given by

$$\varphi(h) = 1, \qquad \text{for all} \quad h \in H,$$

and by

$$\begin{aligned} 7(h) &= 1, && \text{if} \quad h \in L, \\ &= -1, && \text{if} \quad h \in H \backslash L. \end{aligned}$$

Let $x_1, \ldots, x_n$ be coset representatives of $H$ in $G$. The permutation representation of $G$ is the induced representation $\varphi^G$. If $y \in G$ then the $ij$th entry of the matrix $\varphi^G(y)$ is given by

$$\begin{aligned} (\varphi^G(y))_{ij} &= 1, && \text{if} \quad Hx_i y = Hx_j, \\ &= 0, && \text{otherwise.} \end{aligned}$$

The $ij$th entry of the matrix $7^G(y)$ is given by

$$\begin{aligned} (7^G(y))_{ij} &= 7(x_i y x_j^{-1}), && \text{if} \quad Hx_i y = Hx_j, \\ &= 0, && \text{otherwise.} \end{aligned}$$

We see that for every $y \in G$ we have $7^G(y) = D(y)\,\varphi^G(y)$, where $D(y)$ is a diagonal matrix with all diagonal entries $\pm 1$.

We consider $\varphi^G$ as a representation over the complex numbers $\mathbb{C}$. Since $G$ is doubly transitive, $V_n(\mathbb{C})$ breaks into two distinct irreducible subspaces [3-4.3.4]. These are $\langle \mathbf{1} \rangle = \{\lambda(1,..., 1): \lambda \in \mathbb{C}\}$ and its orthogonal complement $\langle \mathbf{1} \rangle^{\perp} = \{(a_1,..., a_n): \sum_{i=1}^{n} a_i = 0\}$.

The following theorem is contained in [4] as Lemma 2.3 and in [17] as Theorem 6.1. We include it here to make our work self-contained.

THEOREM 2.1. *The representation $7^G$ has two distinct irreducible constituents if and only if elements of $L$ are not conjugate in $G$ to elements of $H \backslash L$.*

*Proof.* The norm of a representation $\psi$ of $G$ is defined by

$$\langle \psi, \psi \rangle = 1/|G| \sum_{y \in G} |T_r \psi(y)|^2.$$

Since $\varphi^G$ has two distinct irreducible constituents, $\langle \varphi^G, \varphi^G \rangle = 2$ [3-4.2]. If $y \in G$ then $|T_r \varphi^G(y)| \geqslant |T_r 7^G(y)|$ and so

$$\begin{aligned} 2 &= 1/|G| \sum_{y \in G} |T_r \varphi^G(y)|^2 \\ &\geqslant 1/|G| \sum_{y \in G} |T_r 7^G(y)|^2 \\ &= \langle 7^G, 7^G \rangle. \end{aligned}$$

Either $7^G$ is irreducible or it has two distinct irreducible constituents. If $7^G$ is not irreducible then for any $y \in G$ the diagonal entries of $7^G(y)$ all have the same sign. Let $gyg^{-1}$ be a conjugate of $y$ lying in $H$. Now $g = hx_k$ for some $h \in H$ and some $k = 1,..., n$. Thus $gyg^{-1} = hx_k y x_k^{-1} h^{-1}$ and

$$7(gyg^{-1}) = 7(x_k y x_k^{-1}) = (7^G(y))_{kk}.$$

We see that $gyg^{-1}$ is in $L$ or in $H \backslash L$ according as the diagonal entries of $7^G(y)$ are all 1 or all $(-1)$. Reversing the argument shows that if elements of $L$ are not conjugate to elements of $H \backslash L$ then $7^G$ has norm 2 and so has two distinct irreducible constituents.

For the remainder of this section we assume that elements of $L$ are not conjugate in $G$ to elements of $H \backslash L$.

It is convenient to determine the effect of changing the coset representatives of $H$ in $G$. Let $z_i = h_i x_i$, where $h_i \in H$ and $i = 1,..., n$. If $x_i y x_j^{-1} \in H$ then $x_i y = (x_i y x_j^{-1})\, x_j$ and

$$z_i y = h_i x_i y x_j^{-1} x_j = (h_i x_i y x_j^{-1} h_j^{-1})\, z_j,$$

where $h_i x_i y x_j^{-1} h_j^{-1} \in H$. The matrix of $\varphi^G(y)$ with respect to $z_1,..., z_n$ is the same as the matrix of $\varphi^G(y)$ with respect to $x_1,..., x_n$. The matrix of $7^G(y)$ with respect to $z_1,..., z_n$ is $DAD^{-1} = DAD$, where $A$ is the matrix of $7^G(y)$ with respect to $x_1,..., x_n$ and $D = \mathrm{diag}[7(h_1),..., 7(h_n)]$. If we can find the matrix of $7^G(y)$ with respect to one set of coset representatives then we can easily find the matrix of $7^G(y)$ with respect to other sets of coset representatives.

If $G$ has a normal subgroup $M$ of index two for which $M \cap H = L$, the representation $7^G$ is easy to describe and does not provide interesting subspaces. As $G$ is doubly transitive, $M$ is transitive. This means coset representatives $x_1,..., x_n$ can be chosen from $M$. Now if $x_i y x_j^{-1}$ is in $H$, $7(x_i y x_j^{-1})$ is $-1$ if and only if $y$ is in $G - M$. Thus $7^G$ is the representation obtained from $\varphi^G$ by negating all matrices in $G - M$. The invariant subspaces are again $\langle \mathbf{1} \rangle$ and $\langle \mathbf{1} \rangle^{\perp}$. An example of this ocurs in $S_n$. We assume throughout this section that $G$ does not have such a normal subgroup.

As a consequence of this assumption and the Focal Subgroup Theorem [3, Sect. 7.3], $|\Omega|$ must be even. For if $|\Omega|$ is odd, a Sylow 2-group $S$ of $G$ is contained in $H$. Now $S_1 = S \cap L$ has index two in $S$ and elements of $S - S_1$ are not conjugate to elements of $S_1$ and so the Focal Subgroup of $S$ is contained in $S_1$. By the Focal Subgroup Theorem [3, Sect. 7.3], $G$ has a normal subgroup $M$ if index two such that $H \cap M = L$, which we are assuming is not the case. Now $H$ acts transitively on the odd set $|\Omega - \{a\}|$ and so $L$ acts transitively as well.

We first choose coset representatives so that when the representation $7^G$ is restricted to $H$ it has a simple form. Since $G$ is doubly transitive, $|G|$ is even and we can find an involution $\tau$ not in $H$. This choice of an involution is not essential but it makes later work cleaner. Let $(a)\tau = b$. If $c \in \Omega - \{a\}$ then since $L$ is transitive on $\Omega - \{a\}$ there exists $h_c \in L$ satisfying $(b) h_c = c$. We set $h_b = e$ and we note that the elements $e$, $\tau h_c$, $c \in \Omega - \{a\}$ are coset representatives of $H$ in $G$.

LEMMA 2.2. *If $h \in H$ then the matrix of $7^G(h)$ with respect to the above coset representatives is given by*

$$7^G(h) = 7(h)\, \varphi^G(h).$$

*Proof.* We note that $eh = he$.

If $c \in \Omega - \{a\}$ then $\tau h_c h \in H \tau h_d$, where $d = (c)h$. Now $\tau h_c h = (\tau h_c h h_d^{-1} \tau)\, \tau h_d$ and $\tau h_c h h_d^{-1} \tau \in H$. Since elements of $L$ are not conjugate to elements of $H - L$ and since $h_c$, $h_d \in L$ we have

$$7(\tau h_c h h_d^{-1} \tau) = 7(h_c h h_d^{-1}) = 7(h).$$

This proves the lemma.

We now use a different set of coset representatives to discuss $7^G(\tau)$. Recall that $7^G(\tau)$ is a matrix of the form $D\varphi^G(\tau)$ with $D$ a diagonal matrix with entries $\pm 1$. Let $K = G_{\{a,b\}} = H_{\{b\}}$ be the stabilizer in $G$ of the two points $a$, $b$ of $\Omega$. Suppose $\Delta$ is an orbit of $\Omega$ under $K$. Suppose $c$ and $d$ are both in $\Delta$ with $c' = (c)\tau$ and $d' = d(\tau)$. We will find a set of coset representatives for which the $(c, c')$ entry is the same as the $(d, d')$ entry. For these coset representatives, the entire matrix $7^G(\tau)$ is determined once $\varphi^G(\tau)$ and the signs corresponding to the $(c, (c)\tau)$ positions for one representative of each orbit under $K$ have been determined.

As $\tau$ normalizes $K$, $\tau$ permutes the orbits of $K$. Let $\Delta' = \Delta\tau$. Suppose first that $\tau$ fixes no points of $\Delta$. Let $h_c$, $h_c'$ be elements of $H$ with $bh_c = c$, $bh_c' = c'$. Let $k_d$ be an element of $K$ with $ck_d = d$. Let $k_d' = \tau k_d \tau$; $k_d'$ is in $K$ and $c'k_d' = d'$. Now $bh_c k_d = d$ and $bh_c' k_d' = d'$. With respect to the coset representatives $\tau h_c$ and $\tau h_c'$, the $(c, c')$ entry of $7^G(\tau)$ is $7(\tau h_c \tau (h_c')^{-1}\tau)$. With respect to the coset representatives $\tau h_c k_d$ and $\tau h_c' k_d'$, the $(d, d')$ entry of $7^G(\tau)$ is

$$7(\tau h_c k_d \tau (k_d')^{-1}(h_c')^{-1}\tau) = 7(\tau h_c \tau h_c')^{-1}\tau).$$

This means the signs of these two entries are the same. If $\Delta \neq \Delta'$ choose an element $k_d$ for each $d$ in $\Delta - \{c\}$ and use the coset representatives $\tau h_c$, $\{\tau h_c k_d\}$ for $\Delta$ and the representatives $\tau h_c'$, $\{\tau h_c' \tau k_d \tau\}$ for $\Delta'$. The action of $7^G(\tau)$ mapping $\Delta$ to $\Delta'$ is plus or minus the permutation action of $\varphi^G(\tau)$, the sign being $7(\tau h_c \tau (h_c')^{-1}\tau)$. If $\Delta = \Delta'$, choose an element $k_d$ for each $\tau$-orbit $\{d, d'\}$ in $\Delta - \{c, c'\}$. Use the coset representatives $\tau h_c$, $\tau h_c'$, $\{\tau h_c k_d\}$, $\{\tau h_c' \tau k_d \tau\}$ for $\Delta$. The action of $7^G(\tau)$ mapping $\Delta$ to $\Delta$ is again plus or minus the permutation action of $\varphi^G(\tau)$, the sign again being $7(\tau h_c \tau (h_c')^{-1}\tau)$.

Suppose now that $\Delta\tau = \Delta$ and $\Delta$ contains a point $c$ fixed by $\tau$. Again let $h_c$ be an element of $H$ with $(b)\,h_c = c$. The $(c, c)$ entry of $7^G(\tau)$ has sign $-1$ if and only if $\tau h_c \tau h_c^{-1}\tau$ is in $H - L$. This is clearly when $\tau$ is conjugate to an element of $H - L$. The sign is 1 if it is conjugate to an element of $L$. Now if $d$ is in $\Delta$ let $k_d$ be an element of $K$ mapping $c$ to $d$. Suppose $d\tau = d$. Let $k_d' = k_d$. Now the $(d, d)$ entry of $7^G(\tau)$ has sign $-1$ if and only if $\tau h_c k_d \tau d_k^{-1} h_c^{-1}\tau$ is in $H - L$ which occurs when $\tau$ is conjugate to an element of $H - L$. If $d\tau = d'$ with $d' \neq d$ choose coset representatives $\tau h_c k_d$ and $\tau h_c \tau k_d \tau$. The sign of the $(d, d')$ entry of $7^G(\tau)$ is $7(\tau h_c k_d \tau\tau (k_d)^{-1}\tau h_c^{-1}\tau) = 7(\tau h_c \tau h_c^{-1}\tau)$ which is again $-1$ when $\tau$ is conjugate to an element of $H - L$. For these coset representatives, the sign of $7^G(\tau)$ restricted to $\Delta$ is always $\pm\varphi^G(\tau)$ restricted to $\Delta$, the sign being $-1$ if $\tau$ is conjugate to an element of $H - L$ and $+1$ if $\tau$ is conjugate to an element of $L$.

We have outlined procedures above for finding $7^G$. One choice gives the matrices $7^G|_H$ a particularly nice form in terms of $\varphi^G|_H$; the other gives $7^G(\tau)$ a nice form. Changing from one choice of coset representatives to another involves conjugating by a diagonal matrix with entries $\pm 1$. The $-1$ entries correspond to the positions of coset representatives $\tau h$ in the second set for which $h$ is in $H-L$.

We conclude this section by finding the two irreducible subspaces invariant under $7^G$. We determine two vectors $x, y \in V_n(\mathbb{C})$ and show that one subspace is spanned by the images of $x$ under $7^G$ and the other subspace is spanned by the images of $y$ under $7^G$. Order the basis of $V_n(\mathbb{C})$ by $[a, b$, points in $\Omega - \{a, b\}]$.

We suppose that coset representatives have been chosen so that if $h \in H$ then $7^G(h) = 7(h)\,\varphi^G(h)$. Let $U$ and $W$ be the two irreducible invariant subspaces. By the Frobenius Reciprocity Theorem [3-4.4], $7^G|_H$ has 7 as a constituent with multiplicity 2. Furthermore $U$ and $W$ have unique 1-dimensional subspaces which are invariant under $7^G|_H$, and for which $7^G|_H$ restricted to these subspaces gives the representation 7 of $H$. Let $V$ be the 2-dimensional subspace spanned by $(1, 0, ,\ldots, 0)$ and $(0, 1, 1,\ldots, 1)$. This subspace is invariant under $7^G|_H$ and the restriction of $7^G|_H$ to $V$ has 7 as constituent with multiplicity 2. We have shown that $\dim U \cap V = \dim W \cap V = 1$. Since $U, W \neq V_n(\mathbb{C})$ we may assume that $U \cap V$ is spanned by $(r, 1,\ldots, 1)$ and that $W \cap V$ is spanned by $(s, 1,\ldots, 1)$. Since the matrices in $7^G(G)$ are unitary, $U$ and $W$ are orthogonal and $rs + (n-1) = 0$. The vector

$$(r, 1,\ldots, 1)\, 7^G(\tau) = (1, r, \pm 1,\ldots, \pm 1)$$

is in $U$ and so is orthogonal to $(s, 1,\ldots, 1)$. Suppose there are $u$ plus signs and $w$ minus signs and let $f = u - w$. Then $r + s + f = 0$. Solving for $r$ gives

$$r = \frac{-f \pm \sqrt{[f^2 + 4(n-1)]}}{2},$$

and the two solutions give the values of $r$ and $s$.

The numbers $r$ and $s$ are eigenvalues of an incidence matrix of a graph on $\Omega$ defined by $G$. This graph has been described by Taylor [17]. He defines the graph in terms of the centralizer algebra of $7^G(G)$. His Theorem 6.1 shows that $G$ acts as a group of automorphisms of a regular 2-graph on $\Omega$. We will explicitly construct the graph and show some of its properties.

We begin by determining the centralizer algebra of $7^G(G)$. As this has two distinct irreducible constituents it is spanned by $I$ and another matrix $A$ which we will describe. Let $r_a = (0, 1, 1,\ldots, 1)$, where the columns are labelled by $(a, b, w_3,\ldots, w_n)$, where $a, b, w_3,\ldots, w_n$ are the elements of $\Omega$. Set $a = w_1$ and $b = w_2$. Let $h_i$ be an element of $L$ taking $b$ to $w_i$ for $i = 3, 4,\ldots, n$. Define $r_b = r_a 7^G(\tau)$ and $r_i = r_b 7^G(h_i)$ for $i = 3, 4,\ldots, n$. Recall that if $k$ is in $K = G_{ab}$, $r_b 7^G(k) = 7(k)\, r_b$ and so $r_i$ is well defined. Set $r_1 = r_a$ and $r_2 = r_b$. Let $A$ be the matrix with rows $r_1, r_2, r_3,\ldots, r_n$. Each diagonal entry of $A$ is 0.

The row $r_a$ has $n-1$ entries 1. Each of the remaining rows has a 1 in the $\{a\}$ position, $u$ additional plus signs, and $w$ minus signs. We will show that $A$ commutes with elements of $7^G(G)$.

Suppose first $h$ is in $H$. We showed above that $7^G(h) = 7(h)\,\varphi^G(h)$. Suppose $\varphi(h)$ as a permutation maps $w_i$ to $w_j$. Then the $i$th row of $7^G(h)A$ is $7(h)\,r_j$ as multiplication on the left by $\varphi^G(h)$ maps the $j$th row to the $i$th row. If $i = j = 1$, the first row of $A7^G(h)$ is also $7(h)\,r_i$. For $i \geqslant 2$, the $i$th row of $7^G(h)A$ is $7(h)\,r_j$. The $i$th row of $A7^G(h)$ is

$$r_i 7^G(h) = r_2 7^G(h_i)\,7^G(h) = r_2 7^G(h_i h).$$

But $(b)$ $h_i h = w_j$ and so this is $r_j 7(h)$. This shows $7^G(h)A = A7^G(h)$. To show $7^G(\tau)A = A7^G(\tau)$ notice the first two rows of $7^G(\tau)A$ are $r_2$, $r_1$ and that $r_2 = r_1 7^G(\tau)$ by definition. Clearly $r_1 = r_2 7^G(\tau)$ and so the first two rows of $7^G(\tau)A$ and $A7^G(\tau)$ are equal. Suppose $\tau$ interchanges $w_i$ and $w_j$ with $i, j \geqslant 3$. Now the $i$th row of $7^G(\tau)A$ is $\delta r_j$, where $\delta$ is $7(\tau h_i \tau h_j^{-1}\tau)$. We wish to show $\delta r_j = r_i 7^G(\tau)$. This is equivalent to $\delta r_1 7^G(\tau h_j) = r_1 7^G(\tau h_i \tau)$, which is in turn equivalent to $\delta r_1 = r_1 7^G(\tau h_i \tau h_j^{-1}\tau)$. But $\tau h_i \tau h_j^{-1}\tau$ is in $H$ and so $r_1 7^G(\tau h_i \tau h_j^{-1}\tau) = \delta r_1$. This shows $7^G(\tau)A = A7^G(\tau)$.

We have shown that the centralizer algebra is spanned by $I$ and $A$. As shown in [17, Theorem 6.1], the matrix $A$ is the adjacency matrix of a strong graph $F$. By Proposition 3.2 of [17], the matrix $A$ satisfies the equation $A^2 - fA - (n-1)I = 0$. In the notation of [17], $a = u$, $a^* = w$, and $f = u - w$. The eigenvalues of $-A$ are

$$\tfrac{1}{2}(-f \pm \sqrt{f^2 + 4(n-1)}$$

with multiplicities

$$\tfrac{1}{2}n\{1 \pm f/\sqrt{f^2 + 4(n-1)}\}.$$

Note here

$$n^2 - 4aa^* = f^2 + 4(n-1).$$

There is associated to $F$ a regular 2-graph $\Phi = \delta F$ with parameters as shown. For information about 2-graphs see [13] or [14].

This shows that $r$ and $s$ are the two eigenvalues of $-A$. The invariant subspaces are the different eigenspaces of $-A$. Clearly $(r, 1, \ldots, 1)A = (n-1, * \cdots *)$. As $-rs = n-1$ the vector $(r, 1, \ldots, 1)$ is in the eigenspace of $-A$ with eigenvalue $s$.

*Remarks.* (1) The restriction of the graph $F$ to $\Omega - \{a\}$ is a strongly regular graph with parameters $(v, k, \lambda, \mu)$, where $v = n-1$, $k = w$, $\lambda = 2k - k/2 - n/2$, $\mu = k/2$ [17, Propositions 2.3, 2.4].

(2) We have shown that the representations can be realized over the field $Q(r)=Q(s)$. This is at worst a real quadratic extension of $Q$ and is often $Q$ itself (see [4, Lemma 2.3]).

(3) The parameters of the various doubly transitive groups appear in the Appendix.

## 3. The Hoffman–Singleton Graph and its Automorphism Group

Hoffman and Singleton [8] proved the existence and uniqueness of a strongly regular graph with parameters (50, 7, 0, 1). In this section we construct the Hoffman–Singleton graph according to the prescription given by Shult in [16]. We give a detailed description because we shall need to compute within this graph in later sections.

The Hoffman–Singleton graph, which we denote HS, is a graph on 50 vertices with 175 edges. We describe HS in terms of the alternating group $A_6$ acting on six points 1,..., 6. The group $A_6$ contains 12 subgroups isomorphic to $A_5$ and these fall into two conjugacy classes $C_1$ and $C_2$ each of size 6. The subgroups $M_1,..., M_6$ fixing the points 1,..., 6, respectively, form the class $C_1$. The group $A_6$ admits an involutory outer automorphism $\sigma$ which maps $M_1,..., M_6$ onto $N_1,..., N_6$ in some order. The subgroups $N_1,..., N_6$ form the class $C_2$ and the subgroups $N_j$ do not fix a point. There are 36 Sylow 5-subgroups of $A_6$ and each Sylow 5-subgroup lies in just one group from $C_1$ and one from $C_2$. The Sylow 5-subgroup contained in $M_i$ and in $N_j$ is denoted $P_{ij}$.

Figure 1 shows a skeleton of the graph HS. The vertices labelled 1,..., 6 correspond to the subgroups $M_1,..., M_6$, respectively, and the vertices labelled $1',..., 6'$ correspond to the subgroups $N_1,..., N_6$, respectively. We have arranged the 36 Sylow 5-subgroups in a $6 \times 6$ grid and we list one 5-cycle from each subgroup. The vertex $i$ is joined by edges denoted $O_{ij}$ to each of the six subgroups $P_{ij}$, $j=1,..., 6$, in row $i$ that are contained in $M_i$. The vertex $j'$ is joined by edges denoted $D_{ij}$ to each of the six subgroups $P_{ij}$, $i=1,..., 6$, that are contained in $N_j$. The notation is chosen to conform to the mnemonic that $O_{ij}$ joins $i$ over to $P_{ij}$ and $D_{ij}$ joins $j'$ down to $P_{ij}$. Each vertex $P_{ij}$ is joined to $i$, to $j'$ and by edges called wires to five other vertices $P_{kl}$ in the grid. We now describe the wires.

Two Sylow 5-subgroups $P_{ij}$ and $P_{kl}$ are joined if they do not lie in a common subgroup in $C_1$ or $C_2$ and if there exists an involution in $A_6$ normalizing both $P_{ij}$ and $P_{kl}$. We check that this defines a system of 90 wires and that each subgroup $P_{ij}$ is wired to just five other subgroups $P_{kl}$ in the grid. There are 45 involutions in $A_6$, and since all are conjugate, any involution normalizes the same number of Sylow 5-subgroups. Since the

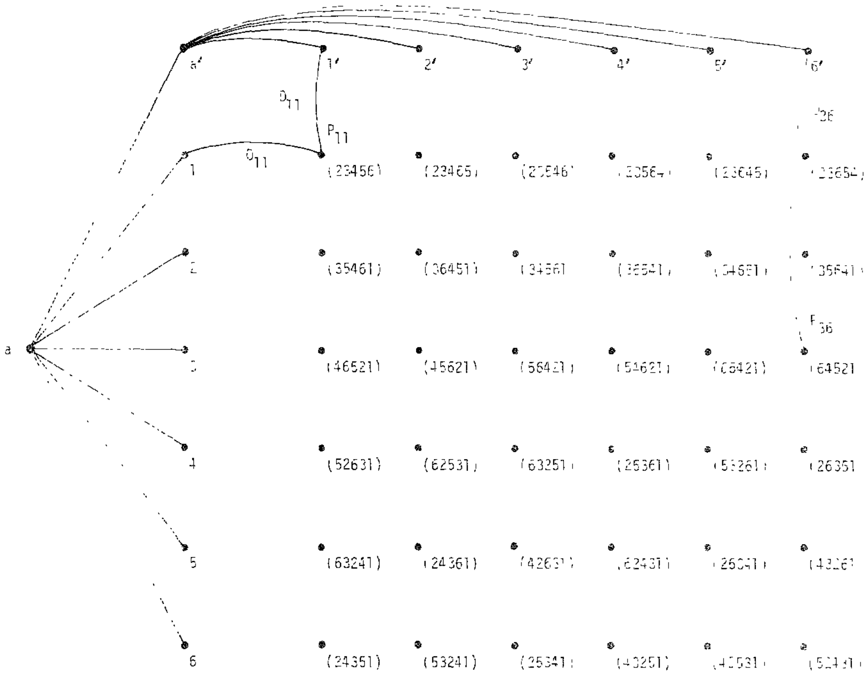
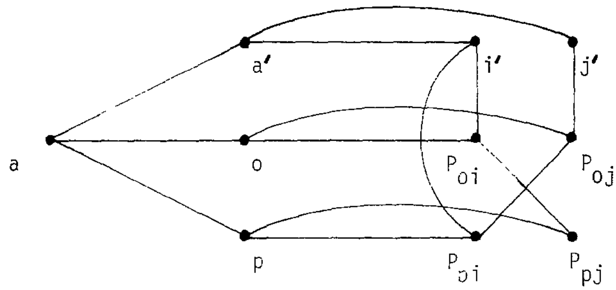


FIGURE 1

normalizer of each Sylow 5-subgroup in $A_6$ is a dihedral group of order 10, each Sylow 5-subgroup is normalized by five involutions. It follows that any involution normalizes exactly four Sylow 5-subgroups. The involution $\lambda = (lm)(kn)(o)(p)$ is the unique involution which normalizes the four Sylow 5-subgroups represented by $(klmno)$, $(kmlno)$, $(klmnp)$ and $(kmlnp)$. The first two subgroups are in row $p$ and the last two subgroups are in row $o$. The automorphism $\sigma$ fixes some involution in $A_6$. After conjugation we may suppose $\sigma$ fixes $\lambda$ and the four Sylow 5-subgroups normalized by $\lambda$ are permuted by $\sigma$. If we set $\{N_{i'}, N_{j'}\} = \{M_o\sigma, M_p\sigma\}$ then two of these subgroups are in $N_{i'}$ and two are in $N_{j'}$. Since $(klmno)^{-1}(klmnp)^2 = (ko)(lmnp)$, we have $\langle(klmno), (klmnp)\rangle \cong A_6$ and $(klmno)$ is joined to $(klmnp)$. Similarly $(kmlno)$ is joined to $(kmlnp)$. It follows that $(klmno)$ and $(kmlnp)$ are in the same column and $(klmnp)$ and $(kmlno)$ are in the same column. Without loss of generality we have the subgraph at the top of the next page. Note this is a Petersen graph. We call the wire $P_{oi}P_{pj}$ the cross of the wire $P_{pi}P_{oj}$. The discussion shows that each subgroup $P_{ij}$ is wired to just five other subgroups $P_{kl}$ as required. Conjugation by $(klmno)^i$ reveals that $(klmno)$ is joined to $(klmnp)$, $(klmpo)$, $(klpno)$, $(kpmno)$ and $(plmno)$. Using this simple rule it is easy to find the five subgroups $P_{kl}$ joined to a given subgroup $P_{ij}$.




We now discuss automorphisms of this graph. Any automorphism $\gamma$ of $A_6$ determines an automorphism of the graph. This automorphism fixes or interchanges $a$ and $a'$ according as $\gamma$ fixes or interchanges the conjugacy class $C_1$ and $C_2$. Thus, the automorphism group of the graph contains a subgroup $K \cong \mathrm{Aut}(A_6)$. The action of $K$ on vertices of HS has orbits $\{a, a'\}$, $\{1,..., 6, 1',..., 6'\}$, and $\{P_{ij}\colon 1 \leqslant i, j \leqslant 6\}$. We now exhibit an automorphism $\alpha$ of HS that fuses these orbits.

The automorphism $\alpha$ fixes $a$, 2, 3, 4, 5, 6, interchanges the pairs $(a', 1)$, $(1', P_{11})$, $(2', P_{12})$, $(3', P_{13})$, $(4', P_{14})$, $(5', P_{15})$, $(6', P_{16})$ and maps $(lmno1)$ to $(lnmo1)$. The map $(lmno1) \to (lnmo1)$ does not depend on the representative of the Sylow 5-subgroup as, for example,

$$\langle (lmno1) \rangle = \langle (moln1) \rangle \to \langle (mlon1) \rangle = \langle (lnmo1) \rangle.$$

Note that $(lmno1)$ is in the same row as $(lnmo1)$. The wire connecting $(lmno1)$ and $(kmno1)$ is mapped by $\alpha$ to the wire connecting $(lnmo1)$ and $(knmo1)$ and so $\alpha$ preserves wires not involving the first row of the grid. We set $P_{1j} = (klmno)$ and we consider the edge connecting $P_{1j}$ and $(klmn1)$. Now $\alpha(P_{1j}) = j'$ and $\alpha((klmn1) = (kmln1)$. Recall that in the discussion above we proved that $(kmln1)$ and $(klmno)$ lie in the same column. Thus $\alpha$ maps wires involving the first row to edges of the form $D_{hk}$, where $h \neq 1$. Clearly $\alpha$ preserves the edges $\{O_{ij} \cup (a'j')\}$. It is now clear that $\alpha$ is indeed an automorphism of HS.

It follows that the automorphism group, Aut(HS), acts transitively on the 50 vertices of HS. In turn, HS is strongly regular with parameters $(50, 7, 0, 1)$. The stabilizer of the vertex $a$ is a subgroup isomorphic to $S_7$. A straightforward argument shows that only the identity fixes $a$, $a'$, 1, 2,..., 6. This means $|\mathrm{Aut(HS)}| = 50.7!$. This group which we denote by $H$ is isomorphic to $P\Gamma U(3, 5)$ as shown in [5]. The representation is of rank 3 on the 50 points.

For future reference we give the action of a specific outer automorphism, $\sigma$, of $A_6$. This automorphism interchanges the pairs $(a, a')$, $(1, 1')$, $(2, 3')$, $(3, 2')$, $(4, 4')$, $(5, 6')$ and $(6, 5')$. This determines the action of $\sigma$ on all subgroups $P_{ij}$. If $\sigma(i)=k'$ and $\sigma(j')=l$ then $\sigma(P_{ij})=P_{lk}$. Note that there are six fixed points $P_{11}$, $P_{23}$, $P_{32}$, $P_{44}$, $P_{56}$ and $P_{65}$.

Finally we describe a graph $\Gamma$ with vertex set the 175 edges of HS. The group $H$ acts transitively on the edges of HS and the stabilizer of the edge $\{a, a'\}$ is the subgroup $K \cong \mathrm{Aut}(A_6)$. We join two vertices in $\Gamma$ if the corresponding edges have distance 2. It is well known (see [9]) that this construction yields a strongly regular graph with parameters (175, 72, 20, 36). This also follows easily from our analysis.

## 4. 100 Cocliques of Size 15 in the Hoffman–Singleton Graph

In Section 3 we constructed the Hoffman–Singleton graph HS and described its automorphism group $H$. In this section we use the structure of $H$ to prove the existence of 100 cocliques of size 15 in HS and to determine how these cocliques intersect.

The group $H$ is isomorphic to $P\Gamma U(3, 5)$ and contains a subgroup $L$ of index 2 that is isomorphic to $PSU(3, 5)$. The stabilizer in $L$ of a vertex in HS is isomorphic to $A_7$ and is maximal in $L$. This gives a conjugate class $\Omega_1$ of 50 subgroups isomorphic to $A_7$. The group $L$ admits an outer automorphism of order 3 that cannot be realized as an automorphism of the graph HS. [3]. The automorphism as a map of $PSU(3, 5)$ is conjugation by the matrix

$$\begin{matrix} w & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix},$$

where $w \neq 1$ is a cube root of 1 in $GF(25)$. It follows that there are two further conjugate classes $\Omega_2$ and $\Omega_3$ each containing 50 subgroups isomorphic to $A_7$. Generators for one of these are listed at the end of this section. Let $T \in \Omega_i$ for $i=2$ or 3 and consider the action of $T$ on the 50 vertices of HS. Since $T$ does not fix a vertex there are two orbits, $D$ and $D'$, of sizes 15 and 35, respectively. This can be seen by considering the possible actions of $A_7$ on 50 points with the elements of orders 3, 5 and 7 fixing the appropriate numbers of points.

Lemma 4.1. *The orbit $D$ is a coclique in HS.*

*Proof.* Let $u, v \in D$ and suppose that $u$ and $v$ are joined. The group $T$ acts transitively on $D$ and if $T_u$ is the stabilizer in $T$ of $u$ then $T_u \cong PSL(3, 2)$. This follows as $|T_u| = |A_7|/15 = 168$. As $T_u \subseteq T$ and $T \cong A_7$, an easy check of conjugate classes shows $T_u$ is simple and is isomorphic to $PSL(3, 2)$. An element of order 7 in $T_u$ acts on $D$ and the orbit sizes must be 1, 7, and 7. It follows that the seven vertices joined to $u$ in HS are all contained in $D$. Since $T$ acts transitively on $D$ every vertex in $D$ is joined to 7 other vertices in $D$. This is impossible because the graph HS is connected. We conclude that $D$ is a coclique in HS.

Let $\Delta_i$, $i = 2, 3$, be the set of 50 cocliques obtained from the conjugate class $\Omega_i$. The cocliques are distinct because each coclique is an orbit of a maximal subgroup of $L$. Each vertex of HS is in 15 cocliques of $\Delta_2$ and 15 cocliques of $\Delta_3$. We shall now determine how the cocliques intersect. The subgroup $T$ acts on $\Delta_i$ and there are three orbits $\{D\}$, 0, and 0′ of sizes 1, 7, and 42, respectively. This follows as $T$ is the image under an automorphism of the stabilizer of a point in $\Omega$ and this stabilizer has orbits of sizes 1, 7, 42 on $\Omega$.

LEMMA 4.2. (1) *If* $E \in 0$ *then* $|D \cap E| = 0$.

(2) *If* $F \in 0'$ *then* $|D \cap F| = 5$.

*Proof.* Let $d \in D$ and $d' \in D'$. Let $u$ and $v$ be the number of cocliques in 0 containing $d$ and $d'$, respectively. Since $T$ acts transitively on $D$ and $D'$ the parameters $u$ and $v$ do not depend on the choice of $d$ and $d'$. Counting incidences of vertices in HS and cocliques in 0 gives $15u + 35v = 7.15$. The possible solutions are $u = 0$, $v = 3$, and $u = 7$, $v = 0$. If $u = 7$ then every coclique in 0 is equal to $D$, which is a contradiction. Thus $u = 0$ and $v = 3$.

Let $|D \cap E| = e$ and $|D \cap F| = f$. Since $T$ acts transitively on 0 and 0′ the parameters $e$ and $f$ do not depend on the choice of $E$ and $F$. Since $u = 0$, we have $e = 0$. Counting incidences of vertices in $D$ and cocliques in 0′ gives $42f = 15.14$. Thus $f = 5$.

We may construct a graph with vertex set $\Delta_i$, $i = 2, 3$, by joining two cocliques $A$, $B \in \Delta_i$ iff $|A \cap B| = 0$. We remark that this graph is a Hoffman–Singleton graph.

The subgroup $T$ acts on $\Delta_j, j \neq i$ and there are two orbits $P$ and $P'$ of sizes 15 and 35, respectively. This can be seen directly as with $T$ acting on $\Omega$ or by utilizing the automorphisms of $L$.

LEMMA 4.3. (1) *If* $M \in P$ *then* $|D \cap M| = 8$.

(2) *If* $Z \in P'$ *then* $|D \cap Z| = 3$.

*Proof.* Let $|D \cap M| = m$ and let $|D \cap Z| = n$. Since $T$ acts transitively on $P$ and $P'$ the parameters $m$ and $n$ do not depend on the choice of $M$ and $Z$.

Again let $d \in D$ and $d' \in D'$. Let $x$ and $y$ be the number of cocliques in $P$ containing $d$ and $d'$, respectively. The argument used in Lemma 4.2 gives $15x + 35y = 15.15$. The possible solutions are $x = 15$, $y = 0$; $x = 8$, $y = 3$; and $x = 1$, $y = 6$. If $x = 15$ then every coclique in $P$ is equal to $D$, which is impossible. Suppose $x = 1$ and $y = 6$. Counting incidences of vertices in $D$ and cocliques in $P$ gives $15m = 15.1$ and so $m = 1$. Counting incidences of vertices in $D$ and cocliques in $P'$ gives $35n = 15.14$ and so $n = 6$. Let $A$, $B \in P$ and suppose $|A \cap B| = 0$. Then the argument used in Lemma 4.1 shows that the seven cocliques in $\Delta_j$ disjoint from $A$ are all contained in $P$. If $C \in P$, if $B \neq C$, and if $|A \cap C| = 0$ then by Lemma 4.2

$$\begin{aligned} |(A \cup B \cup C) \cap D'| &= 3\,|A \cap D'| - |B \cap C \cap D'| \\ &\geqslant 42 - 5 \\ &> |D'|, \end{aligned}$$

which is impossible. We conclude that two cocliques in $P$ cannot be disjoint. Since $T$ acts transitively on $P'$ every coclique in $P'$ is disjoint from three cocliques in $P$. Let $R \in P'$, let $S_i \in P$, $i = 1, 2, 3$, and suppose $|R \cap S_i| = 0$, $i = 1, 2, 3$. Then inclusion–exclusion gives

$$\begin{aligned} |(R \cup S_1 \cup S_2 \cup S_3) \cap D'| &\geqslant |R \cap D'| + 3\,|S_1 \cap D'| - 3\,|S_1 \cap S_2| \\ &\geqslant 9 + 3.14 - 3.5 \\ &> |D'|, \end{aligned}$$

which is impossible. We conclude $x = 8$ and $y = 3$. It follows that $m = 8$ and $n = 3$.

In Fig. 2 we list a coclique $D$ and a representative coclique from each of the orbits 0, 0′, $P$ and $P'$. In Fig. 2, (124) denotes the graph automorphism

| | |
|---|---|
| $D$ | $a, 5', 6', P_{11}, P_{12}, P_{21}, P_{24}, P_{33}, P_{34}, P_{41}, P_{43}, P_{52}, P_{54}, P_{62}, P_{63}$ |
| $E = D\sigma\alpha$ | $1', 3', 4', 1, 5, 6, P_{22}, P_{25}, P_{26}, P_{32}, P_{35}, P_{36}, P_{42}, P_{45}, P_{46}$ |
| $F = D(124)$ <br> $= D(1'5'6')(2'3'4')$ | $a, 1', 6', P_{14}, P_{15}, P_{23}, P_{25}, P_{32}, P_{34}, P_{42}, P_{45}, P_{52}, P_{53}, P_{63}, P_{64}$ |
| $M = D\sigma\alpha\sigma$ | $1, 2, 4, 1', 5', 6', P_{32}, P_{33}, P_{34}, P_{52}, P_{53}, P_{54}, P_{62}, P_{63}, P_{64}$ |
| $Z = D(13)(26)(45)$ <br> $= D(5'6')$ | $a, 5', 6', P_{13}, P_{14}, P_{22}, P_{23}, P_{31}, P_{32}, P_{42}, P_{44}, P_{51}, P_{53}, P_{61}, P_{64}$. |

FIG. 2. Representative cocliques from HS. Note: $|D \cap E| = 0$, $|D \cap F| = 5$, $|D \cap M| = 8$, $|D \cap Z| = 3$. Here $D$, $E$, $F$ are in $\Delta_2$ and $M$, $Z$ are in $\Delta_3$.

determined by the automorphism of $A_6$ that is conjugation by (124). The following automorphisms fix the coclique $D$;

$$\begin{aligned} g_1 &= (1, 2, 3, 4, 5, 6)\alpha \\ &= (a)(a'1, 2, 3, 4, 5, 6)(5'P_{11}, P_{21}, P_{34}, P_{41}, P_{52}, P_{63}) \\ &\quad (6'P_{12}, P_{24}, P_{33}, P_{43}, P_{54}, P_{62})\ldots, \\ g_2 &= (124)(365), \\ g_3 &= (13)(45), \\ g_4 &= (456)\sigma\alpha\sigma(46) \\ &= (a6'5')(P_{11}, P_{63}, P_{41}, P_{33}, P_{21}, P_{43})(P_{12}, P_{24}, P_{52}, P_{34}, P_{62}, P_{54})\ldots, \end{aligned}$$

where the automorphisms $\sigma$ and $\alpha$ are described in Section 3. The group

$$S = \langle g_1, g_2, g_3\rangle \cong PSL(3, 2).$$

The group

$$T = \langle g_i \colon i = 1, 2, 3, 4\rangle \cong A_7.$$

An easy check shows $T$ is transitive on $D$ with $T_a = S$.

The incidence matrices for these two families of cocliques provide examples of matrix equations studied by Ryser in [12]. Let $A$ be the incidence matrix for the cocliques in $\Delta_2$ and $B$ the incidence matrix for the cocliques in $\Delta_3$. In each case the columns are labelled by the 50 vertices of HS and the rows are labelled by the cocliques in $\Delta_2$ or $\Delta_3$. A given entry $(Y, X)$ is 1 if the vertex $X$ is in the coclique $Y$ and 0 otherwise. Each row of $A$ and $B$ has 15 1's and 35 0's. Each row in $A$ has inner product 0 with seven rows and has inner product 5 with the remaining distinct rows. The graph obtained by joining two rows if they are orthogonal gives a Hoffman–Singleton graph. The vertices correspond to a family of 50 conjugate subgroups $H_1,\ldots, H_{50}$ in $PSU(3, 5)$. Each $H_i$ is isomorphic to $A_7$. There is an automorphism $\beta$ of order two which takes the subgroups $H_i$ to the subgroups $L_i$ which define the cocliques in $\Delta_2$. Suppose $H_i$ stabilizes the point $i$. Then a point $j$ is in the coclique defined by $L_i$ if and only if $j$ is in the orbit of size 15 of $L_i$ acting on $1, 2,\ldots, 50$. This occurs when $|(L_i)_j| = 168$, which is equivalent to $|L_i \cap H_j| = 168$. But $|L_i \cap H_j| = 168$ implies $|H_i \cap L_j| = 168$ as $\beta(L_i) = H_i$ and $\beta(H_j) = L_j$. This shows that the map $\beta'$ of $\{i\}$ to the coclique defined by $\beta(H_i) = L_i$ is a polarity. Consequently, the cocliques can be ordered so that $A$ is symmetric. The same is true for $B$.

Suppose $A$ and $B$ are symmetric. In the notation of [12, Sect. 2] with $A = X = Y$ our computations show

$$A^2 = AA^T = A^TA = 15I + 0E + 5F$$
$$= 15I - 5E + 5J.$$

The parameters of these equations are as follows:

$$\lambda = 0, \qquad \mu = 5, \qquad a = 15, \qquad b = -5, \qquad \sigma = 40, \qquad \rho = 225.$$

Note $AA^T = A^TA$ and $(\sigma, \lambda - \mu) = 5$ (cf. [12, Theorem 2.1]). The matrix $B$ satisfies the same conclusion. Furthermore $AB$ has all entries 3 or 8. Each row and column has 15 entries 8 and 35 entries 3.

## 5. A Monomial Representation of the Higman–Sims Group

In Section 3 we introduced a strongly regular graph $\Gamma$ with parameters $(175, 72, 20, 36)$. The vertices of $\Gamma$ are the 175 edges of the Hoffman–Singleton graph HS and two edges are joined if they have distance 2. The automorphism group of $\Gamma$ contains the automorphism group $H$ of the graph HS. Shult [16] constructs a doubly transitive group $G$ acting on 176 points in which the stabilizer of a point acts on the remaining points in a manner permutation-isomorphic to $H$ acting on the vertices of $\Gamma$. The group $H$ is isomorphic to $P\Gamma U(3, 5)$ and contains a subgroup $L$ of index 2 that is isomorphic to $PSU(3, 5)$. Furthermore elements of $L$ are not conjugate in $G$ to elements of $H \backslash L$. We shall apply the method described in Section 2 to construct a monomial representation $7^G(G)$ of $G$ of degree 176 with two distinct irreducible constituents. There are two invariant subspaces $C$ and $C^\perp$ of dimensions 22 and 154, respectively. We shall exhibit 100 vectors in $C$ that are permuted by the matrices in $7^G(G)$. This provides a natural proof that $G$ is isomorphic to the primitive permutation group of degree 100 constructed by Higman and Sims in [6]. (See [15].) These different permutation representations are evident by viewing $G$ as a subgroup of Conway's group .0 [2]. Shult gives a different argument in [16].

Let $\Omega$ be the set consisting of a point $\infty$ together with the 175 vertices of $\Gamma$. The group $H$ acts transitively on $\Omega \backslash \{\infty\}$ and $G = \langle H, \tau \rangle$, where $\tau$ is the arc-breaking map described by Shult in [16]. The map $\tau$ interchanges $\infty$ and $\{a, a'\}$, fixes the 12 edges $\{a, i\}$, $\{a', i'\}$, where $i = 1,..., 6$, interchanges $D_{ij}$ and $0_{ij}$ for $i, j = 1,..., 6$, and interchanges a wire $w$ and its cross $w^*$. If $K = G_{\infty\{a,a'\}}$ then $K \cong \mathrm{Aut}(A_6)$ since $K$ is the stabilizer in $H$ of an edge in HS.

Lemma 5.1. *The involution $\tau$ centralizes $K$.*

*Proof.* If $k \in K$ then it is clear that $\tau k = k\tau$ when restricted to $\infty$, $\{a, a'\}$ and to $\{a, i\}$, $\{a', i'\}$ for $i = 1,..., 6$. If $k(P_{ij}) = P_{rs}$ and $k(a) = a$,

$$\tau k(D_{ij}) = \tau(D_{rs}) = 0_{rs} = k(0_{ij}) = k\tau(D_{ij})$$

and a similar argument shows $\tau k(0_{ij}) = k\tau(0_{ij})$. The case $k(a) = a'$ is handled similarly. Let $w_i$, $i = 1, 2$ be a wire and let $w_i^*$ be its cross. If $k(w_1) = w_2$, it is easy to see using the description of the cross involving the Petersen graph that $k(w_1^*) = w_2^*$ and we have

$$\tau k(w_1) = \tau(w_2) = w_2^* = k(w_1^*) = k\tau(w_1).$$

This proves the lemma.

We now describe the representation $7^G$ obtained by inducing the alternating character of $H$ to $G$. The orbits of $K$ on $\Omega$ are $\infty$, $\{a, a'\}$, $\{\{a, i\}, \{a', i'\}; i = 1,..., 6\}$, $\{D_{ij}, 0_{ij}; i, j = 1,..., 6\}$ and $\{w: w \text{ is a wire}\}$. In Section 2 we showed that the signs of the non-zero entries of $7^G(\tau)$ can be determined by computing the sign of a single entry in each orbit of $K$. We remark that all involutions in $L$ fix 16 points in $\Omega$ and are conjugate to (12) (34). All involutions in $H \backslash L$ fix 12 points in $\Omega$ and are conjugate to (12) or $\sigma$.

LEMMA 5.2. *If $t$ is an involution in $K' \cong A_6$, then $t\tau$ fixes 12 points of $\Omega$.*

*Proof.* If $t$ is an involution in $K'$, then $t$ is determined by the inner automorphism of $A_6$ that is conjugation by some $(kl)(mn)$, say. The product $t\tau$ fixes the edges $\{a, o\}$, $\{a, p\}$, $\{a', i'\}$ and $\{a', j'\}$, where $o, p$ are the fixed points of $t$ on $\{1, 2,..., 6\}$ and $i', j'$ are the fixed points of $t$ on $\{1', 2',..., 6'\}$. Any other fixed point under $t$ is a wire. The wire $w$ is fixed by $t\tau$ exactly when $t$ interchanges $w$ and its cross $w^*$. If this happens, $(kl)(mn)$ must centralize the involution in $A_6$ corresponding to the pair $w$, $w^*$ in Section 3. Consequently that involution is one of $(km)(ln)$, $(kn)(lm)$, $(kl)(op)$, or $(mn)(op)$ as these are the only involutions in $A_6$ other than $(kl)(mn)$ centralizing $(kl)(mn)$. The involution could not be $(kl)(mn)$ as it fixes both $w$ and $w^*$. Hence there are at most eight fixed wires. Since $t\tau$ fixes at most 12 points it fixes exactly 12 points. In particular, the crosses determined by the four involutions found above are interchanged by $t$.

Let $S$ be a set of 45 wires with the property that if a wire $w$ is in $S$ then its cross $w^*$ is not. The proof of Lemma 2 reveals that given a wire $w$ there is an involution $t_w$ in $K \cap L$ that interchanges $w$ and its cross $w^*$. Given $w \in S$ there is an element $l_w \in L$ such that $l_w(\{a, a'\}) = w$. The set $\{\tau l_w, \tau l_w t_w; w \text{ in } S\}$ is a set of coset representatives for the $K$-orbit of wires. The sign of $7^G(\tau)$ on this orbit is $7(\tau l_w \tau t_w l_w^{-1} \tau)$. By Lemma 5.2 this sign is $(-1)$.

The element $\sigma$ of $H$ is determined by an outer automorphism of $A_6$ and is described in Section 3.

LEMMA 5.3. *The element $\tau\sigma$ fixes 12 points of $\Omega$.*

*Proof.* Let $w = \{P_{ij}, P_{kl}\}$ be a wire and let $w^* = \{P_{il}, P_{kj}\}$ be its cross. If $\tau\sigma$ fixes $w$, then $\sigma$ interchanges $w$ and $w^*$. If $\sigma(P_{ij}) = P_{il}$ then $\sigma$ fixes $\langle P_{ij}, P_{il}\rangle \cong A_5$ and if $\sigma(P_{ij}) = P_{kj}$ then $\sigma$ fixes $\langle P_{ij}, P_{kj}\rangle \cong A_5$. But $\sigma$ interchanges the two conjugate classes of such subgroups and so cannot fix one. We conclude that $\tau\sigma$ does not fix a wire.

If $\sigma(P_{ij}) = P_{rs}$ then $\tau\sigma(D_{ij}) = \tau(0_{rs}) = D_{rs}$ and $\tau\sigma(0_{ij}) = 0_{rs}$. As shown in Section 3, $\sigma$ fixes six Sylow 5-subgroups. The element $\tau\sigma$, then, fixes 12 edges of the form $D_{ij}$ or $0_{ij}$. Finally the points $\infty$, $\{a, a'\}$ and $\{a, i\}$, $\{a', i'\}$, for $i = 1,..., 6$, are not fixed by $\tau\sigma$ and so $\tau\sigma$ fixes 12 points of $\Omega$.

To determine the appropriate sign for the $\{D_{ij} \cup 0_{ij}\}$ orbit, choose one of the points $P_{ij}$ fixed by $\sigma$. For definiteness, choose $P_{11}$. Let $h$ be an element of $L$ mapping $\{aa'\}$ to $0_{11}$. Now $h' = h\sigma$ maps $\{aa'\}$ to $D_{11}$. As $\sigma$ is in $H-L$, $h\sigma$ is also in $H-L$. Now $7(\tau h\tau(h')^{-1}\tau) = 7(\tau h\tau\sigma h^{-1}\tau)$. As $\tau\sigma$ fixes 12 points, this sign is $-1$. There are elements $l_{ij}$ in $L \cap K$ mapping $P_{11}$ to $P_{ij}$. Choose as coset representatives $\tau h l_{ij}$ and $\tau h' l_{ij}$. With respect to these coset representatives, the action of $7^G(\tau)$ restricted to $\{D_{ij} \cup 0_{ij}\}$ is $-\varphi^G(\tau)$ restricted to $\{D_{ij} \cup 0_{ij}\}$. Denote this matrix $S$. Note that each of the coset representatives of the form $\tau h l_{ij}$ has $h l_{ij}$ in $L$ and each of the coset representatives of the form $\tau h' l_{ij}$ has $h' l_{ij}$ in $H-L$. If we now choose a basis for which all coset representatives of the form $\tau h$ have $h$ in $L$, the matrix $S$ is replaced by a matrix $DSD$, where $D$ is a diagonal matrix indexed by $\{D_{ij} \cup 0_{ij}\}$ with $-1$ entries in the $(D_{ij}, D_{ij})$ positions and $+1$ entries in the $(0_{ij}, 0_{ij})$ positions. This means $S$ is replaced by $-S$ and with respect to these coset representatives, $7^G(\tau)$ restricted to $\{D_{ij} \cup 0_{ij}\}$ is the same as $\varphi^G(\tau)$.

The remaining orbit is the set $\{\{ai\}, \{a'i'\};\ i = 1, 2,..., 6\}$. As $\tau$ fixes every one of these, the argument in Section 2 shows $7^G(\tau)$ negates each of these points as $\tau$ is conjugate to an element of $H-L$. We have now computed $7^G(\tau)$ completely.

Given a matrix $C$ in $7^G(G)$ we write $M \to \pm N$ according as the $M$, $N$th entry of $C$ is $\pm 1$. We have

THEOREM 5.4. *There exists a set of coset representatives of $H$ in $G$ such that*

(1) $7^G(h) = 7(h)\,\varphi^G(h)$ *if* $h \in H$, *and*

(2) *the matrix of* $7^G(\tau)$ *is given by*

 (i) $\infty \to \{a, a'\}$,

 (ii) $\{a, a'\} \to \infty$,

(iii) $D_{ij} \to 0_{ij}$,

(iv) $0_{ij} \to D_{ij}$,

(v) $\{a, i\} \to -\{a, i\}$,

(vi) $\{a', i'\} \to -\{a', i'\}$,

(vii) $w \to -w^*$, *where $w$ is a wire and $w^*$ its cross.*

*Proof.* Take the set of coset representatives, $e$, $\tau$, $\{\tau h\}$ with $h$ in $L$ described above.

We are now able to produce the two invariant subspaces $C$ and $C^*$ as in Section 2. Here $u = 72$, $w = 102$, $f = -30$, $n = 176$. Now

$$\sqrt{f^2 + 4(n-1)} = \sqrt{900 + 700} = 40.$$

The eigenvalues $r$ and $s$ are $(30 + 40)/2 = 35$ and $(30 - 40)/2 = -5$, respectively. The multiplicities are $88(1 - (30/40)) = 22$ and $88(1 + (30/40)) = 154$. The 22-dimensional space is spanned by $(-5, 1, \ldots, 1)$ and its images; the 154-dimensional space is spanned by $(35, 1, \ldots, 1)$ and its images. Let $C$ be the 22-dimensional space and let $C^*$ the 154-dimensional space.

We now introduce 100 vectors in the code $C$ and we shall prove that these vectors are permuted by the matrices in $7^G(G)$.

If $A$ is a coclique in $\Delta_2$ define a vector $V_A$ by

$$\begin{aligned}(V_A)_E &= \phantom{-}1 && \text{if } E = \infty\\ &= -1 && \text{if } E \text{ is an edge involving a vertex of } A\\ &= \phantom{-}1 && \text{otherwise.}\end{aligned}$$

If $A$ is a coclique in $\Delta_3$ define a vector $V_A$ by

$$\begin{aligned}(V_A)_E &= -1 && \text{if } E = \infty\\ &= \phantom{-}1 && \text{if } E \text{ is an edge involving a vertex of } A\\ &= -1 && \text{otherwise.}\end{aligned}$$

This defines a set $\Lambda$ of 100 vectors. If we can prove $\Lambda 7^G(G) = \Lambda$ then $\Lambda$ spans an invariant subspace of dimension less than 154 and so $\Lambda \subseteq C$. If $h \in L$ then $7^G(h) = \varphi^G(h)$ and $V_A 7^G(h) = V_{h(A)}$. If $h \in H \backslash L$ then $7^G(h) = -\varphi^G(h)$, $h(\Delta_2) = \Delta_3$, and $V_A 7^G(h) = V_{h(A)}$. This proves $H$ preserves $\Lambda$ and it remains to check that $7^G(\tau)$ preserves $\Lambda$.

LEMMA 5.5. *The group $K$ acts on $\Lambda$ and there are two orbits $S$ and $S'$. The orbit $S$ consists of the 40 vectors $V_A$ corresponding to cocliques $A$ that* *do not contain $a$ or $a'$. The orbit $S'$ consists of the* 60 *vectors $V_B$ corresponding to cocliques $B$ that contain one of $a$ and $a'$.*

*Proof.* Let $M$ be the coclique described in Section 4 and let $Y = M(1325)(46) = M(1'3'6'4')(2'5')$. In Fig. 3 vertices in $M$ are denoted $\bullet$ and vertices in $Y$ are denoted $*$. Note that $M$ is determined by 1, 2, 4, 1′, 5′, 6′ and that $Y$ is determined by 3, 5, 6, 2′, 3′, 4′. Note that $M, Y \in \Delta_3$ and that $M$, $Y$ do not contain $a$ or $a'$. Given $\{d, e, f\} \subseteq \{1, 2, 3, 4, 5, 6\}$ there is a graph automorphism $h$ in $K'$ with $h(\{1, 2, 4\}) = \{d, e, f\}$. Recall $K' \cong A_6$. It follows that there are at least $\binom{6}{3} = 20$ cocliques in $\{Mk: k \in K'\}$.

Now let $N = M(12) = M(1'3')(2'5')(4'6')$. Note that $N$ contains $\{1, 2, 4\}$ in common with $M$. The entries in the top row and in rows 3, 5, 6 of $N$ to the right of the $a'$ column are the complements of the entries of these rows in $M$. This applies to each of the 20 cocliques found above and so there are at least 40 such cocliques.

Let $D$ and $Z$ be the cocliques described in Section 4. In Fig. 4 vertices in $D$ are denoted $\bullet$ and vertices in $Z$ are denoted $*$. Note that $D \in \Delta_2$, $Z \in \Delta_3$ and $D$, $Z$ both contain $a$. Given $\{d', e'\} \subseteq \{1', 2', 3', 4', 5', 6'\}$ there is a graph automorphism $h$ in $K$ with $h(a) = a$ and $h(\{5', 6'\}) = \{d', e'\}$. It follows that there are at least $\binom{6}{2} = 15$ pairs of cocliques in $\{DK: k \in K\}$ that contain $a$. Since $\sigma \in K$ and since $\sigma(a) = a'$ there are at least 60 vectors in $\{Dk: k \in K\}$. This completes the proof.

By Lemma 5.1 the involution $\tau$ centralizes $K$. If $V \in \Lambda$ and if $V7^G(\tau) \in \Lambda$ then for all $k \in K$ the vector

$$(V7^G(k)\, 7^G(\tau)) = (V7^G(\tau)\, 7^G(k))$$

is also in $\Lambda$. If we can prove that $V_M 7^G(\tau) \in \Lambda$ and $V_D 7^G(\tau) \in \Lambda$ then it will follow that $7^G(\tau)$ preserves $\Lambda$.

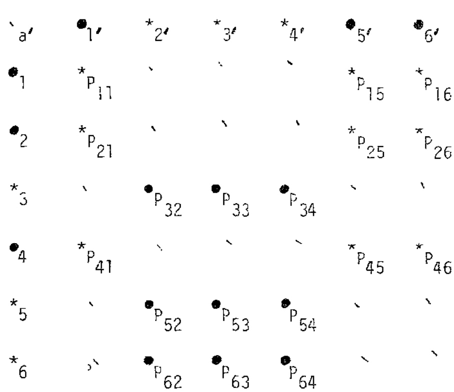



FIG. 3. The cocliques $M$ and $Y$. Vertices in $M$ are denoted by $\bullet$; those in $Y$ are denoted by $*$.

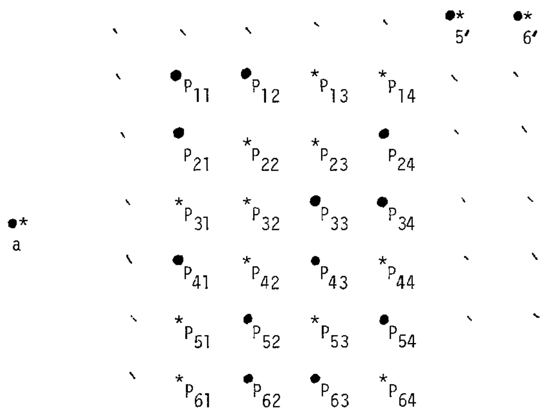



FIG. 4. The cocliques $D$ and $Z$. Vertices in $D$ are denoted by $\bullet$; those in $Z$ are denoted by $*$.

LEMMA 5.6. *We have* $V_M 7^G(\tau) = V_Y$.

*Proof.* The action of the matrix $7^G(\tau)$ is described in Theorem 5.4 and the entries of $V_M$ and $V_Y$ are listed in Fig. 5. This table can be read directly from Fig. 3 with the exception of the wires joining points of $M$ or of $Y$. As $M$ and $Y$ are cocliques, there are no wires joining points of $M$ or of $Y$. Consequently, the wires from the points of $M$ in rows 3, 5, 6 to points in rows 3, 5, 6 must all go to columns 1′, 5′, 6′. In particular, each $P_{ij}$ in rows 3, 5, 6 not in $M$ is wired to two elements in $M$ in each of the two rows other than $i$ containing entries from $M$. In particular there are no wires connecting points in rows 3, 5, 6 and columns 1′, 5′, 6′. The lemma is proved by checking the entries of $V_Y$ listed in a given row are obtained from the entries of $V_M$ listed in the same row by applying the matrix $7^G(\tau)$. For example, it must be checked that crosses of wires joined to points of $M$ are not joined to points of $Y$ and the crosses of wires not joined to points of $M$ are joined to points of $Y$. As $M$ and $Y$ are both in $\Delta_3$, $V_M 7^G(\tau) = VY$.

LEMMA 5.7. *We have* $V_D 7^G(\tau) = V_Z$.

*Proof.* The entries of $V_D$ and $V_Z$ are listed in Fig. 6 and the lemma is proved in the same way as Lemma 5.6. The only tricky part is to check those entries indexed by wires. We see from Fig. 4 again as no points of $D$ or $Z$ are joined that any wire $w = \{P_{ij}, P_{kl}\}$, where $j$, $l = 1, 2, 3, 4$ must contain one vertex from $D$ and one vertex from $Z$. The $w$th entry of $V_D$ is $(-1)$. Applying $7^G(\tau)$ gives the same set of wires but changes each entry from $(-1)$ to 1. It remains to show that given a wire $w = \{P_{ij}, P_{kl}\}$ with $P_{ij} \in D$ and $l = 5, 6$ then its cross $w^* = \{P_{il}, P_{kj}\}$ satisfies $P_{kj} \in Z$. Suppose $P_{kj} \in D$. We

| Entries in $V_M$ | | Entries in $V_Y$ | |
|---|---|---|---|
| 1 | -1 | 1 | -1 |
| | $\infty$<br>$\{a,a'\}$ | | $\{a,a'\}$<br>$\infty$ |
| $\{a,i\}$, $i=1,2,4$<br>$\{a',i'\}$, $i=1,5,6$ | $\{a,i\}$, $i=3,5,6$<br>$\{a',i'\}$, $i=2,3,4$ | $\{a,i\}$, $i=3,5,6$<br>$\{a',i'\}$, $i=2,3,4$ | $\{a,i\}$, $i=1,2,4$<br>$\{a',i'\}$, $i=1,5,6$ |
| $O_{1j},O_{2j},O_{4j}$, $j=1,\ldots,6$<br>$O_{3j},O_{5j},O_{6j}$, $j=2,3,4$<br>$D_{i1},D_{i5},D_{i6}$, $i=1,\ldots,6$<br>$D_{i2},D_{i3},D_{i4}$, $i=3,5,6$ | all other edges of type $D_{ij},O_{ij}$. | $D_{1j},D_{2j},D_{4j}$, $j=1,\ldots,6$<br>$D_{3j},D_{5j},D_{6j}$, $j=2,3,4$<br>$O_{i1},O_{i5},O_{i6}$, $i=1,\ldots,6$<br>$O_{i2},O_{i3},O_{i4}$, $i=3,5,6$ | all other edges of type $D_{ij},O_{ij}$. |
| $\{P_{ij},P_{k\ell}\}$ $i=3,5,6$ $j=2,3,4$ | all other wires | all other wires | $\{P_{i\ell},P_{kj}\}$ $i=3,5,6$ $j=2,3,4$<br>(these are crosses of wires in the left hand box of this row) |

FIG. 5. The vectors $V_M$ and $V_Y$.

see from Fig. 4 that there is a column $s$ with $P_{is}$, $P_{ks} \in Z$. Let $P_{ms}$ be the remaining entry in the $s$th column in $Z$. Recall that $P_{ij}$ is wired to some entry in the $s$th column. It cannot be $P_{is}$ nor can it be $P_{ks}$ since $P_{ij}$ is wired to $P_{kl}$. Therefore $P_{ij}$ is wired to $P_{ms}$. In the same way $P_{kj}$ is also wired to $P_{ms}$. Since $j'$ is the unique point joined to $P_{ij}$ and $P_{kj}$, this is impossible. The lemma now follows.

We have now proved

THEOREM 5.8. *The* 100 *vectors in* $A$ *are contained in* $C$ *and are permuted by the matrices in* $7^G(G)$.

It is now straightforward to check that $7^G(G)$ acts as a rank 3 permutation group on these vectors. The stabilizer of a point is a subgroup isomorphic to $M_{22}$ which acts on orbits of sizes 1, 22, 77. The action on 22 points is the natural action of $M_{22}$ on 22 points.

LEMMA 5.9. *There are two possible inner products of distinct vectors* $\langle V_X, V_Y\rangle$, *where* $X$, $Y$ *are distinct cocliques. These values are* 64 *and* $-16$. *The group isomorphic to* $M_{22}$ *acts transitively on the* 176 *points in a rank* 3 *manner with orbits of size* 1, 105, 70.

| Entries in $V_D$ | | Entries in $V_Z$ | |
|---|---|---|---|
| 1 | −1 | 1 | −1 |
| $\infty$ | $\{a, a'\}$ | $\{a, a'\}$ | $\infty$ |
| $\{a', i'\}$, $i = 1, \ldots, 4$ | $\{a, i\}$, $i = 1, \ldots, 6$<br>$\{a', i'\}$, $i = 5, 6$ | $\{a, i\}$, $i = 1, \ldots, 6$<br>$\{a', i'\}$, $i = 5, 6$ | $\{a', i'\}$, $i = 1, \ldots, 4$ |
| $O_{ij}$, $j = 5, 6$<br>$O_{ij}$, $D_{ij}$, $P_{ij} \notin D$<br>and $j = 1, 2, 3, 4$ | $D_{ij}$, $j = 5, 6$<br>$O_{ij}$, $D_{ij}$, $P_{ij} \in D$<br>and $j = 1, 2, 3, 4$ | $D_{ij}$, $j = 5, 6$<br>$O_{ij}$, $D_{ij}$, $P_{ij} \in Z$<br>and $j = 1, 2, 3, 4$ | $O_{ij}$, $j = 5, 6$<br>$O_{ij}$, $D_{ij}$, $P_{ij} \notin Z$<br>and $j = 1, 2, 3, 4$ |
| all other wires | $\{P_{ij}, P_{k\ell}\}$, $j, \ell = 1, 2, 3, 4$<br>$\{P_{ij}, P_{k\ell}\}$, $P_{ij} \in D$<br>and $\ell = 5, 6$ | $\{P_{i\ell}, P_{kj}\}$ $j, \ell = 1, 2, 3, 4$<br>$\{P_{i\ell}, P_{kj}\}$, $P_{kj} \in Z$<br>and $\ell = 5, 6$ | all other wires |

FIG. 6. The vectors $V_D$ and $V_Z$.

## 6. A BINARY CODE PRESERVED BY THE HIGMAN–SIMS GROUP

In Section 5 we described a monomial representation $7^G$ of the Higman–Sims group $G$ and we examined the 22-dimensional subspace $C$ that is preserved by $7^G(G)$. This representation can be reduced modulo any prime and in this section we consider the reduction modulo 2. We obtain a binary $[176, 22, 50]$ code $C_2$ containing exactly 176 vectors of minimum weight 50. The support of a vector of minimum weight is a block in a symmetric 2-(176, 50, 14) design. G. Higman constructs a symmetric 2-(176, 50, 14) design in [7] and proves that the automorphism group of this design is the Higman–Sims group.

The subspace $C$ contains the following vectors

(1) $(V_g \pm V_h)/2$, for all $g, h \in G$, where $V_1 = (-5, 1, \ldots, 1)$ and $V_g = V_1 7^G(g)$.

(2) $(V_A \pm V_B)/2$, for all $V_A, V_B \in \mathcal{A}$, where $V_A$ is the vector corresponding to the coclique $A$.

(3) $(V_A \pm V_g)/2$, for all $g \in G$ and for all $V_A \in \mathcal{A}$.

If $x$ is a vector listed above then each entry of $x$ is an integer. We reduce each entry modulo 2 and we regard $x$ as a vector in $\mathbb{F}_2^{176}$. Let $C_2$ be the subspace of $\mathbb{F}_2^{176}$ spanned by the vectors listed above. Then $\dim(C_2) \leqslant 22$.

We reduce the entries of the matrices in $7^G(G)$ modulo 2 and obtain a permutation group which we denote by $G_2$. Note that $G_2$ preserves $C_2$.

We have found 22 independent vectors in the code $C_2$, 21 of type (2) and one of type (3), and so we have $\dim(C_2)=22$. The weight distribution of $C_2$ was computed by N. J. A. Sloane. The number $A_i$ of codewords of weight $i$ in $C_2$ is listed in Fig. 7.

Since $G_2$ acts 2-transitively on the coordinate positions, the support of a vector of minimum weight is a block in a symmetric 2-(176, 50, 14) design.

We do need a computer to calculate the weight distribution of $C_2$. However we can obtain many properties of the code $C_2$ by hand.

Let $U$ be the subspace of $C_2$ spanned by the vectors $(V_A \pm V_B)/2$ for $V_A$, $V_B \in \Lambda$. By Lemma 5.9 we have $V_R \cdot V_S = 176$, 64 or $-16$ for all $V_R$, $V_S \in \Lambda$. Hence $U$ is self-orthogonal.

We now describe a subspace $V$ of $U$ that is preserved by a subgroup of $G_2$ that is isomorphic to $M_{22}$. In Fig. 2 of Section 4 we listed the vertices of the graph HS that are contained in the cocliques $D$, $E$ and $M$. There are 7 cocliques $E_1=E, E_2,\ldots, E_7$ in $\Delta_2$ that are disjoint from $D$ and there are 15 cocliques $M_1=M, M_2,\ldots, M_{15}$ in $\Delta_3$ that meet $D$ in eight vertices. Let $W_i=(V_D+V_{E_i})/2$, for $i=1,\ldots,7$, and let $W_{i+7}=(V_D+V_{M_i})/2$, for $i=1,\ldots,15$. The vectors $W_j$, $j=1,\ldots,22$, are permuted by a subgroup of $7^G(G)$ that is isomorphic to $M_{22}$. By Lemma 5.9 this subgroup acts transitively on the 176 coordinate positions. We reduce each vector $W_j$ modulo 2 and we let $V$ be the subspace of $C_2$ spanned by these vectors. For each coordinate $E$ we define $B(E)=\{W_i\colon (W_i)_E=1\}$. The binary vectors $W_1,\ldots, W_{22}$ are permuted by a subgroup $M$ of $G_2$ that is isomorphic to $M_{22}$.

LEMMA 6.1. *Every vector $W_i$, $i=1,\ldots,22$, has weight* 56.

The sets $B(E)$ are the 176 blocks of a Steiner 4-(23, 7, 1) system that miss a given point.

| | |
|---|---|
| $A_0 = A_{176} = 1$ | $A_{72} = A_{104} = 15400$ |
| $A_{50} = A_{126} = 176$ | $A_{78} = A_{98} = 193600$ |
| $A_{56} = A_{120} = 1100$ | $A_{80} = A_{96} = 604450$ |
| $A_{64} = A_{112} = 4125$ | $A_{82} = A_{94} = 462000$ |
| $A_{66} = A_{110} = 5600$ | $A_{86} = A_{90} = 369600$ |
| $A_{70} = A_{106} = 17600$ | $A_{88} = 847000$ |

FIG. 7. Weight distribution of codewords in $C_2$.

*Proof.* Since $M$ acts transitively on $W_1,\ldots, W_{22}$, we only need to calculate $wt(W_8)$. Since $W_8 = (V_D + V_M)/2$ we have

$$wt(W_8) = \text{the number of entries where } V_D \text{ and } V_M \text{ agree.}$$

The entries of the vectors $V_D$ and $V_M$ are listed in Figs. 5 and 6 of Section 4. A direct check gives $wt(W_8) = 56$.

Since $M$ acts transitively on the sets $B(E)$, every set $B(E)$ contains the same number $k$ of vectors $x_i$. Counting pairs $(W_i, E)$, where $(W_i)_E = 1$, gives $22.56 = 176k$, and so $k = 7$. Since $M$ acts 3-transitively on $W_1,\ldots, W_{22}$, a counting argument shows any three distinct vectors are contained in four sets $B(E)$. We shall prove that $|B(E) \cap B(F)| = 1$ or 3. It then follows easily that the sets $B(E)$ are the 176 blocks of a Steiner 4-(23, 7, 1) system that miss a given point.

It can be shown the group $M_\infty$ is the stabilizer in Aut(HS) of the coclique $D$ and there are three orbits of coordinate positions. These are $\{\infty\}$, $0 = \{E: E$ is an edge of HS involving $D\}$, and $0' = \{E: E$ is not an edge of HS involving $D\}$. We set $p = |B(\infty) \cap B(E)|$ for $E \in 0$ and we set $q = |B(\infty) \cap B(E)|$ for $E \in 0'$. Counting pairs $(W_i, E)$, where $W_i \in B(\infty)$ and $(W_i)_E = 1$, gives

$$7.56 = 7 + 105p + 70q.$$

The possible solutions are $p = 3$, $q = 1$ and $p = 1$, $q = 4$. If $q = 4$ then there are three vectors in $B(\infty)$ that are contained in at least $70 \times 4/\binom{7}{3} = 8$ sets $B(E)$ in $0'$. This is impossible and we conclude $|B(\infty) \cap B(E)| = 1$ or 3 for all sets $B(E) \neq B(\infty)$. The transitivity of $M$ now gives $|B(E) \cap B(F)| = 1$ or 3 for all sets $B(E) \neq B(F)$.

LEMMA 6.2. *The binary code $V$ is a $[176, 11, 56]$ code with weight distribution*

$$A_0 = A_{176} = 1, \quad A_{56} = A_{120} = 22, \quad A_{80} = A_{96} = \binom{22}{2} \quad \textit{and} \quad A_{88} = \binom{22}{3}.$$

*Proof.* A vector $v = (a_1,\ldots, a_{22})$ in $\mathbb{F}_2^{22}$ determines a codeword $\varphi(v) = \sum_{i=1}^{22} a_i x_i$ in $V$. The map $\varphi$ is a homomorphism and we require the weight distribution of $\varphi(\mathbb{F}_2^{22})$.

We define a Steiner 4-(23, 7, 1) system $S$ by introducing an extra point $x$ and 77 extra blocks $\{x\} \cup T_i$, $i = 1,\ldots, 77$. The 253 vectors which support the blocks of $S$ span the binary Golay code $C_{23}$ [11]. The code $C_{23}$ is a perfect 3-error-correcting [23, 12, 7] code. Given a vector $v \in \mathbb{F}_2^{23}$ there exists a unique codeword $c \in C_{23}$ and a unique vector $e$ of weight 0, 1, 2 or 3 such that $v = c + e$. We take every vector in $\mathbb{F}_2^{23}$ and delete the entry indexed by $x$.

The code $C_{23}$ determines a $[22, 12, 6]$ code $C_{22}$ in this way. It remains true that given a vector $v \in \mathbb{F}_2^{22}$ there exists a codeword $c \in C_{22}$ and a vector $e \in \mathbb{F}_2^{22}$ of weight 0, 1, 2, or 3 such that $v = c + e$. However, if $e$ is a vector of weight 3 in $\mathbb{F}_2^{22}$ then there is a unique vector $e^* \neq e$ in $(\mathbb{F}_2)^{22}$ also of weight 3 such that $e + e^* \in C_{22}$. Note that $C_{22} + e = C_{22} + e^*$. If $e$ and $f$ are distinct vectors of weight at most 2, $C_{22} + e \neq C_{22} + f$.

Since $|B(E) \cap B(F)| = |B(E) \cap T_i| = 1$ or 3, for all coordinates $E$, $F$ and for all $i = 1,\dots, 77$, we have $\varphi(V_{B(F)}) = \varphi(V_{T_i}) = \mathbf{1}$, where $V_{B(F)}$, $V_{T_i}$ are the vectors with support $B(F)$ and $T_i$, respectively. Thus $\varphi(C_{22}) = \{\mathbf{0}, \mathbf{1}\}$ and if $C_{22} + v$ is a coset of $C_{22}$ in $\mathbb{F}_2^{22}$ then $\varphi(C_{22} + v) = \{\varphi(v), \mathbf{1} + \varphi(v)\}$. Furthermore we may take $v$ to be a vector $e$ of weight 0, 1, 2, or 3. The number of cosets of each type is listed in Fig. 8. Since $Z$ acts 3-transitively on $x_1,\dots, x_{22}$ we may define $\lambda_i$, $i \leqslant 3$ to be the number of blocks $B(E)$ containing $i$ distinct vectors from $x_1,\dots, x_{22}$. A counting argument gives $\lambda_1 = 56$, $\lambda_2 = 16$, and $\lambda_3 = 4$. We are now able to calculate $wt(\varphi(e))$, where $e \in \mathbb{F}_2^{22}$ and $wt(e) = 0$, 1, 2 or 3. The results are listed in Fig. 8 and the lemma follows from these results.

Consider the graph automorphism $g_1 = (a)(a'1, 2, 3, 4, 5, 6)$ listed in Section 4, and the graph automorphisms $h_1 = (16)(25)(34) = (1'5')$ and $h_2 = (15)(24)(36) = (4', 5')$. The automorphisms obtained from $g_1$, $h_1$, and $h_2$ in the usual way determine elements of $G_2$ which we also denote by $g_1$, $h_1$, and $h_2$, respectively. Since $g_1$ fixes the coclique $D$ we have $g_1 \in Z$. The element $h_1$ inverts $g_1$; $h_2$ inverts another element of order 7 in the stabilizer of $D$. Since $g_1$ has order 7, it fixes a second coclique $P$ in $\{E_i, M_j;\ i = 1,\dots, 7,\ j = 1,\dots, 15\}$. The element $h_1$ interchanges $D$ and $P$. Note that $h_1$ does not fix $D$ and $P$ because otherwise we would have $g_1$, $h_1$ in $Z$ but $g_1$ is not conjugate to $g_1^{-1}$ in $Z$. The subspace $Vh_1$ is invariant under $h_1 Z h_1$, and $h_1 Z h_1 \cap Z \cong M_{21}$. Since $h_1$ fixes $\mathbf{1}$ and $(V_D + V_P)/2$ we have $\dim(V \cap Vh_1) \geqslant 2$. By considering the possible actions of $M_{21}$ on quotients it can be seen that $\dim(V \cap Vh_1) = 2$ and so $\dim\langle V, Vh_1\rangle = 20$. A similar analysis using $h_2$ shows that $\dim\langle V, Vh_2\rangle = 20$ and that $\dim\langle V, Vh_2\rangle = 21$. Since

| Type of coset $C_{22} + e$ | Number of such cosets | Weight of $\varphi(e)$ |
|---|---|---|
| $e = \underline{0}$ | 1 | 0 |
| $wt(e) = 1$ | 22 | $\lambda_1 = 56$ |
| $wt(e) = 2$ | $\binom{22}{2} = 231$ | $2\lambda_1 - 2\lambda_2 = 80$ |
| $wt(e) = 3$ | $\frac{1}{2}\binom{22}{3} = 770$ | $3\lambda_1 - 6\lambda_2 + 4\lambda_3 = 88$ |

FIGURE 8

$\langle V, Vh_1, Vh_2\rangle \subseteq U$ we have $\dim(U) \geqslant 21$. One may also use Lemma 6.4 below to obtain this.

LEMMA 6.3. *The code $C_2 = \langle U, (V_D + V_1)/2\rangle$, and $C_2$ is self-orthogonal.*

The code $U$ is a doubly even $[176, 21, 56]$ code with all weights divisible by 8. The weight enumerator for each code can be read from Fig. 7.

*Proof.* Since $U$ is self-orthogonal and since $U$ is spanned by vectors of weight divisible by 4 it follows that every vector in $U$ has weight divisible by 4. Now

$$\begin{aligned}(V_D + V_1)_E &= -4 && \text{if } E = \infty\\ &= \ \ 0 && \text{if } E \text{ is an edge involving } D\\ &= \ \ 2 && \text{if } E \text{ is an edge not involving } D\end{aligned}$$

Therefore $wt((V_D + V_1)/2) = 70$ and $(V_D + V_1)/2 \in C_2 \backslash U$. We have $C_2 = \langle U, (V_D + V_1)/2\rangle$ and $\dim(U) = 21$. Now

$$\begin{aligned}V_A \cdot V_1 &= -5 - 35 && \text{if } A \in \Delta_2,\\ &= 5 + 35 && \text{if } A \in \Delta_3.\end{aligned}$$

It follows that $((V_A + V_B)/2) \cdot ((V_D + V_1)/2) \equiv 0 \pmod 2$ and so $C_2$ is self-orthogonal. The weight distribution of $C_2$ and $U$ is contained in Fig. 7.

LEMMA 6.4. *The group $G_2$ acts absolutely irreducibly on $U/\langle(\mathbf{1})\rangle$.*

*Proof.* There are several straightforward ways to see this. One is to restrict the action of $G_2$ to the action of its Sylow 5-group $S$. This is a non-abelian group of order $5^3$ with the element in the center conjugate to all of its non-trivial powers. A faithful representation over a field of characteristic 2 containing a fifth root of 1 has dimension 5. The center is represented by a scalar. Any faithful representation of $G_2$ when restricted to $S$ must contain all four of these constituents and so must have degree at least 20. It follows that $G_2$ acts absolutely irreducibly on $U/\langle(\mathbf{1})\rangle$.

# Appendix

TABLE I

Doubly Transitive Groups for which the Point Stabilizer Has a Subgroup of Index 2 Satisfying the Fusion Condition of Section 2

| Group | $\lvert\Omega\rvert$ | $k$ | $l$ | $\lambda$ | $\mu$ | $\rho_1$ | $\rho_2$ | $f_1$ | $f_2$ |
|---|---|---|---|---|---|---|---|---|---|
| $PSL(2,q)$ <br> $q \equiv 1 \pmod 4$ | $q+1$ | $\frac{q-1}{2}$ | $\frac{q-1}{2}$ | $\frac{q-5}{4}$ | $\frac{q-1}{4}$ | $\sqrt{q}$ | $-\sqrt{q}$ | $\frac{q+1}{2}$ | $\frac{q+1}{2}$ |
| $S_p(2n,2)$ <br> $n \geqslant 3$ <br> (two representations) | $2^{n-1}(2^n \pm 1)$ | $2(2^{n-1} \mp 1)(2^{n-2}+1)$ | $2^{2n-2}$ | $2(2^{n-2} \mp 1)(2^{n-2}+2)$ <br> $+1$ | $(2^{n-1} \mp 1)(2^{n-2} \pm 1)$ | $1 \pm 2^{n-1}$ | $1 \mp 2^n$ | $\frac{2^{2n}-1}{3}$ | $\frac{(2^n \pm 1)(2^{n-1} \pm 1)}{3}$ |
| $PSU(3,q)$ <br> $q$ odd | $q^3+1$ | $\frac{(q-1)(q^2+1)}{2}$ | $\frac{(q+1)(q^2-1)}{2}$ | $\frac{(q-1)^3}{4}-1$ | $\frac{(q-1)(q^2+1)}{4}$ | $q^2$ | $-q$ | $\frac{q^3+1}{q+1}$ | $\frac{(q^3+1)q}{(q+1)}$ |
| $R(q) = {}^2G_2(q)$ <br> $q = 3^{2n+1}$ | $(q^3+1)$ | $\frac{(q-1)(q^2+1)}{2}$ | $\frac{(q+1)(q^2-1)}{2}$ | $\frac{(q-1)^3}{4}-1$ | $\frac{(q-1)(q^2+1)}{4}$ | $q^2$ | $-q$ | $\frac{q^3+1}{q+1}$ | $\frac{(q^3+1)q}{q+1}$ |
| Higman–Sims | 176 | 72 | 102 | 20 | 36 | 35 | $-5$ | 22 | 154 |
| $Co_3 - 1.3$ | 276 | 112 | 162 | 30 | 56 | 55 | $-5$ | 23 | 253 |

*Note.* $\lvert\Omega\rvert$ is the size of $\Omega$ or the index of the stabilizer of a point. The parameters $(\lvert\Omega\rvert - 1, k, l, \lambda, \mu)$ are the parameters of the strongly regular graph as described in Section 2. The values $\rho_1$ and $\rho_2$ are the eigenvalues of the incidence matrix. The multiplicity of $\rho_1$ is $f_1$ and the multiplicity of $\rho_2$ is $f_2$. Note $f_1 + f_2 = \lvert\Omega\rvert$.

## References


1. M. Broué and M. Enguehard, "La geometrie de Graham Higman invariante par le groups d'Higman–Sims," Exposés au Seminaire Claude Chevalley (Avril–Mai 1974).
2. J. H. Conway, Three lectures on exceptional groups, *in* "Finite Simple Groups," pp. 215–247, Academic Press, New York, 1971.
3. D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.
4. M. P. Hale, Jr. and E. E. Shult, Equiangular lines, the graph extension theorem, and transfer in triply transitive groups, *Math. Z.* **135** (1974), 111–123.
5. D. Higman, Finite permutation groups of rank 3, *Math. Z.* **86** (1964), 145–156.
6. D. Higman and C. Sims, A simple group of order 44, 352, 000, *Math. Z.* **105** (1968), 110–113.
7. G. Higman, On the simple group of D. G. Higman and C. C. Sims, *Illinois J. Math.* **13** (1969), 74–80.
8. A. J. Hoffman and R. R. Singleton, On Moore graphs with diameter 2 and 3, *I.B.M. J. Res. Develop.* **4** (1960), 497–504.
9. X. L. Hubaut, Strongly regular graphs, *Discrete Math.* **13** (1975), 357–371.
10. J. H. van Lint and F. J. MacWilliams, Generalized quadratic residue codes, *IEEE Trans. Inform. Theory*, **IT-24**, no. 6 (1978), 730–737.
11. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error Correcting Codes," North-Holland, Amsterdam, 1977.
12. H. J. Ryser, The factors of a design matrix, *J. Combinatorial Theory* **22**, no. 2 (1977), 181–193.
13. J. J. Seidel, A survey of 2-graphs, *in* "Proc. Intern. Colloqu. Teorie Combinatorie (Roma 1973)," Tomo I, pp. 481–511, Acad. Naz. Lincei, 1976.
14. J. J. Seidel and D. E. Taylor, Two-graphs, a second survey, *in* "Proc. Intern. Colloqu., Algebraic Methods in Graph Theory, Szeged 1978," to appear.
15. C. C. Sims, On the isomorphism of two groups of order 44, 352, 000, *in* "Theory of Finite Groups," pp. 101–108, Benjamin, New York, 1969.
16. E. E. Shult, "The Graph Extension Theorem," *Proc. Amer. Math. Soc.* **33** (1972), 278–284; and supplement to "The Graph Extension Theorem," mimeographed notes, University of Florida.
17. D. E. Taylor, Regular 2-graphs, *Proc. London Math. Soc. Ser. 3*, **35** (1977), 257–274.
18. H. N. Ward, Quadratic residue codes and symplectic groups, *J. Algebra* **29** (1974), 150–171.